

ABSTRACT

A method and system for providing a hash and a complement of the hash for an item in a computer system are disclosed. The method and system include providing a plurality of components from the item. The plurality of components include a first component and a last component. Each of the plurality of components includes a particular number of bits. The method and system also include cascading the plurality of components through at least one XOR to provide a plurality of resultants. The plurality of resultants includes a first resultant and a final resultant. The final resultant includes only the last component. The first resultant includes an XOR of the first component and remaining cascaded components of the plurality of components. The method and system also include applying an invertible hash function and an invertible hash function complement to at least the first resultant to provide the hash. The complement of the hash includes the plurality of resultants except the first resultant. In another aspect, the method and system include applying the invertible hash function and its complement to at least the first component of the plurality of components, before the plurality of components are cascaded through the at least one XOR. In this aspect, the hash includes the first resultant. The complement of the hash includes the plurality of resultants except the first resultant.